CLAIMS

We claim:

1. A method of operating a virtual private network (VPN) based on IP Sec that integrates network address translation (NAT) with IP Sec processing, comprising the steps of:

configuring a NAT IP address pool;

configuring a VPN connection to utilize said NAT IP address pool;

obtaining a specific IP address from said NAT IP address pool, and allocating said specific IP address for said VPN connection;

starting said VPN connection;

loading to an operating system kernel the security associations and connection filters for said VPN connection;

processing a IP datagram for said VPN connection; and

applying VPN NAT to said IP datagram.

2. The method of claim 1, wherein said VPN connection is configured for outbound processing, and said applying step comprises outbound source IP Nating.

3. The method of claim 1, wherein said VPN connection is configured for some combination of inbound processing, and said applying step selectively comprises inbound source IP NATing or inbound destination IP NATing.

4. The method of claim 1, further for integration of NAT with IP Sec for manually-keyed IP Sec connections, comprising the further step of manually configuring connection keys.

5. The method of claim 1, further for integrating NAT with IP sec for dynamically-keyed (e.g. IKE) IP Sec connections, comprising the further step of:

configuring the VPN connections to obtain their keys automatically.

6. The method of claim 1, further for integrating NAT with IP Sec Security Associations, negotiated dynamically by IKE, wherein said starting step further comprises creating a message for IKE containing said IP address from said NAT pool; and further comprising the step of operating IKE to obtain dynamically negotiated keys.

7. The method of claim 6, further comprising the step of combining the dynamically obtained keys with said NAT pool IP address and wherein said loading step loads the result as security associations into said operating system kernel.

8. A method for allowing the definition and configuration of NAT directly with definition and configuration of IPsec-based VPN connections and VPN policy, comprising the steps of:

configuring the requirement for VPN NAT by a yes/no decision in a policy database for each of the three types of VPN NAT, said three types being VPN NAT type a

outbound source IP NAT, VPN NAT type c inbound source IP NAT, and VPN NAT type d inbound destination IP NAT; and

configuring a remote IP address pool or a server IP address pool selectively responsive to said yes/no decision for each said VPN NAT type.

9. The method of claim 8, further comprising the step of configuring a unique said remote IP address pool for each remote address to which a VPN connection will be required, whereby said remote IP address pool is keyed by a remote ID.

10. The method of claim 8, further comprising the step of configuring said server IP address pool once for a system being configured.

11. A method of providing customer tracking of VPN NAT activities as they occur in an operating system kernel, comprising the steps of:

responsive to VPN connection configuration, generating journal records;

updating said journal records with new records for each datagram processed through a VPN connection; and

enabling a customer to manage said journal records.

12. A method of allowing a VPN NAT address pool to be associated with a gateway, thereby allowing server load- balancing, comprising the steps of:

configuring a server NAT IP address pool for a system being configured;

storing specific IP addresses that are globally routable in said server NAT IP address pool;

configuring a VPN connection to utilize said server NAT IP address pool; and

managing total volume of concurrent VPN connections responsive to the number of addresses in said server NAT IP address pool.

13. A method of controlling the total number of VPN connections for a system based on availability of NAT addresses, comprising the steps of:

configuring the totality of remote IP address pools with a common set of IP addresses, said addresses being configured as a range, as a list of single addresses, or any combination of multiple ranges and single addresses; and

limiting the successful start of concurrently active VPN connections responsive to the number of said IP addresses configured across the totality of said remote address pools.

14. A method of performing network address translation on selected ICMP datagrams, comprising the steps of:

detecting selected types of ICMP type packets; and

responsive to said selected types, performing network address translation functions on the entire datagram including ICMP data.

15. A method of performing network address translation on selected FTP datagrams, comprising the steps of:

detecting the occurrence of FTP PORT or PASV FTP commands; and

responsive to said command, performing network address translation on the FTP data and the header.

16. A system for operating a virtual private network (VPN) based on IP Sec that integrates network address translation (NAT) with IP Sec processing, comprising:

means for configuring a NAT IP address pool;

means for configuring a VPN connection to utilize said NAT IP address pool;

means for obtaining a specific IP address from said NAT IP address pool, and allocating said specific IP address for said VPN connection;

means for starting said VPN connection;

means for loading to an operating system kernal the security associations and connection filters for said VPN connection;

means for processing a IP datagram for said VPN connection; and

means for applying VPN NAT to said IP datagram.

17. A system for definition and configuration of NAT directly with definition and configuration of VPN connections and VPN policy, comprising:

a policy database for configuring the requirement for VPN NAT by a yes/no decision for each of the three types of VPN NAT, said three types being VPN NAT type a outbound source IP NAT, VPN NAT type c inbound source IP NAT, and VPN NAT type d inbound destination IP NAT; and

a remote IP address pool or a server IP address pool selectively configured responsive to said yes/no decision for each said VPN NAT type.

18. A system for allowing a VPN NAT address pool to be associated with a gateway, thereby allowing server load- balancing, comprising:

a server NAT IP address pool configured for a given system being configured for containing multiple address configured as a range, as a list of single addresses, or any combination multiple ranges and single addresses;

said server NAT IP address pool storing specific IP addresses that are globally routable;

a VPN connection configured to utilize said server NAT IP address pool; and

a connection controller for managing total volume of concurrent VPN connections responsive to the number of addresses in said server NAT IP address pool.

19. A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for operating a virtual private network (VPN) based on IP Sec that

integrates network address translation (NAT) with IP Sec processing, said method steps comprising:

configuring a NAT IP address pool;

configuring a VPN connection to utilize said NAT IP address pool;

obtaining a specific IP address from said NAT IP address pool, and allocating said specific IP address for said VPN connection;

starting said VPN connection;

loading to an operating system kernal the security associations and connection filters for said VPN connection;

processing a IP datagram for said VPN connection; and

applying VPN NAT to said IP datagram.

20. An article of manufacture comprising:

a computer useable medium having computer readable program code means embodied therein for operating a virtual private network (VPN) based on IP Sec that integrates network address translation (NAT) with IP Sec processing , the computer readable program means in said article of manufacture comprising:

computer readable program code means for causing a computer to effect configuring a NAT IP address pool;

computer readable program code means for causing a computer to effect configuring a VPN connection to utilize said NAT IP address pool;

computer readable program code means for causing a computer to effect obtaining a specific IP address from said NAT IP address pool, and allocating said specific IP address for said VPN connection;

computer readable program code means for causing a computer to effect starting said VPN connection;

computer readable program code means for causing a computer to effect loading to an operating system kernal the security associations and connection filters for said VPN connection;

computer readable program code means for causing a computer to effect processing a IP datagram for said VPN connection; and

computer readable program code means for causing a computer to effect applying VPN NAT to said IP datagram.

21. Method for providing IP security in a virtual private network using network address translation (NAT), comprising the steps of:

dynamically generating NAT rules and associating them with manual or dynamically generated (IKE) Security Associations; thereafter

beginning IP security that uses the Security Associations; and then

as IP Sec is performed on outbound and inbound datagrams, selectively performing one or more of VPN NAT type a outbound source IP NAT, VPN NAT type c inbound source IP NAT, and VPN NAT type d inbound destination IP NAT.

22. The method of claim 1, said NAT IP address pool containing multiple addresses configured as a range, as a list of single address, or any combination of multiple ranges and single addresses.